



A new family of maximal curves

Beelen, Peter ; Montanucci, Maria

Published in:
Journal of the London Mathematical Society

Link to article, DOI:
[10.1112/jlms.12144](https://doi.org/10.1112/jlms.12144)

Publication date:
2018

Document Version
Early version, also known as pre-print

[Link back to DTU Orbit](#)

Citation (APA):
Beelen, P., & Montanucci, M. (2018). A new family of maximal curves. *Journal of the London Mathematical Society*, 98(2), 573-592. <https://doi.org/10.1112/jlms.12144>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

A new family of maximal curves

Peter Beelen and Maria Montanucci

Abstract

In this article we construct for any prime power q and odd $n \geq 5$, a new $\mathbb{F}_{q^{2n}}$ -maximal curve \mathcal{X}_n . Like the Garcia–Güneri–Stichtenoth maximal curves, our curves generalize the Giulietti–Korchmáros maximal curve, though in a different way. We compute the full automorphism group of \mathcal{X}_n , yielding that it has precisely $q(q^2 - 1)(q^n + 1)$ automorphisms. Further, we show that unless $q = 2$, the curve \mathcal{X}_n is not a Galois subcover of the Hermitian curve. Finally, up to our knowledge, we find new values of the genus spectrum of $\mathbb{F}_{q^{2n}}$ -maximal curves, by considering some Galois subcovers of \mathcal{X}_n .

2000 MSC: 11G20 (primary), 11R58, 14H05 (secondary)

1 Introduction

Let \mathcal{K} be an absolutely irreducible, non-singular, projective algebraic curve defined over the finite field \mathbb{F}_q with q elements. The famous Hasse–Weil bound states that \mathcal{K} can have at most $q + 1 + 2g(\mathcal{K})\sqrt{q}$ points defined over \mathbb{F}_q , where $g(\mathcal{K})$ denotes the genus of the curve \mathcal{K} . The curve \mathcal{K} is called \mathbb{F}_q -maximal if it attains the Hasse–Weil bound. A curve of genus 0 is “maximal” for any q , but otherwise this can only be the case if the cardinality q of the finite field is a square.

An important and well-studied example of an \mathbb{F}_{q^2} -maximal curve is given by the Hermitian curve \mathcal{H}_q . It is a plane curve, which can be defined by the affine equation

$$\mathcal{H}_q : Y^{q+1} = X^{q+1} - 1.$$

Other equivalent affine equations are often given, such as the equation $Y^{q+1} = X^q + X$, but for our purposes the above equation will be most convenient. For fixed q , the curve \mathcal{H}_q has the largest possible genus $g(\mathcal{H}_q) = q(q-1)/2$ that an \mathbb{F}_{q^2} -maximal curve can have. The automorphism group of \mathcal{H}_q is known to be $PGU(3, q)$, which is a group of order $(q^3 + 1)q^3(q^2 - 1)$. A result commonly attributed to Serre, see [17, Proposition 6], gives that any \mathbb{F}_{q^2} -rational curve which is covered by an \mathbb{F}_{q^2} -maximal curve is itself also \mathbb{F}_{q^2} -maximal. Therefore many maximal curves can be obtained by constructing subcovers of already known maximal curves, in particular subcovers of the Hermitian curve. For a while it was speculated in the research community that perhaps all maximal curves could be obtained as subcovers of the Hermitian curve, but it was shown by Giulietti and Korchmáros that this is not the case; see [10]. More precisely, they constructed an \mathbb{F}_{q^6} -maximal curve which is not a subcover of the Hermitian curve \mathcal{H}_{q^3} . We will denote this \mathbb{F}_{q^6} -maximal curve by \mathcal{C} and call it the Giulietti–Korchmáros (GK) curve. It is defined over \mathbb{F}_{q^6} by the affine equations

$$\mathcal{C} : \begin{cases} Z^{q^2-q+1} = Y \frac{X^{q^2}-X}{X^q+X} \\ Y^{q+1} = X^q + X \end{cases}.$$

The GK curve can be seen as a cover of the Hermitian curve \mathcal{H}_q .

A generalization of \mathcal{C} , often called the Garcia–Güneri–Stichtenoth (GGS) curve or the generalized GK curve, was introduced in [9]. For any prime power q and odd $n \geq 3$, they found an $\mathbb{F}_{q^{2n}}$ -maximal curve \mathcal{C}_n with genus $g(\mathcal{C}_n) = (q-1)(q^{n+1} + q^n - q^2)/2$, given by the affine equations

$$\mathcal{C}_n : \begin{cases} Z^m = Y \frac{X^{q^2} - X}{X^q + X} \\ Y^{q+1} = X^q + X \end{cases},$$

where $m := (q^n + 1)/(q + 1)$. Note that in particular $\mathcal{C} = \mathcal{C}_3$. Moreover, it is known that for any q and $n \geq 5$, the curve is not a Galois subcover of the Hermitian curve \mathcal{H}_{q^n} ; [7, 11]. The automorphism group of \mathcal{C} was determined in [10]. There it was shown that each automorphism of \mathcal{H}_q can be extended to an automorphism of \mathcal{C} in exactly m distinct ways and that each automorphism of \mathcal{C} is obtained in that way. In other words: the automorphism group of \mathcal{H}_q , can be lifted completely and \mathcal{C} has exactly $(q^3 + 1)q^3(q^2 - 1)m$ automorphisms. For $n \geq 5$ a similar statement is not true: it was shown in [13, 14] that only the stabilizer of the infinite point Q_∞ of \mathcal{H}_q can be lifted completely and that any automorphism of \mathcal{C}_n is obtained in this way, yielding $|Aut(\mathcal{C}_n)| = q^3(q^2 - 1)m$. Note that from [16, Theorem A.10] the stabilizer of Q_∞ is a maximal subgroup of $Aut(\mathcal{H}_q) \cong PGU(3, q)$ of order $q^3(q^2 - 1)$.

It is natural to ask whether or not it is possible to construct other generalizations of \mathcal{C} such that other subgroups of $PGU(3, q)$ can be lifted completely. In this article we give a possible answer for the maximal subgroup of $PGU(3, q)$ given by the non-tangent line stabilizer of \mathcal{H}_q . This group has order $(q+1)q(q^2 - 1)$ and permutes the $q+1$ \mathbb{F}_{q^2} -rational points of \mathcal{H}_q lying on the intersection of \mathcal{H}_q with an \mathbb{F}_{q^2} -rational non-tangent line. In the following we construct for each odd $n \geq 5$, an $\mathbb{F}_{q^{2n}}$ -maximal curve \mathcal{X}_n in which precisely this non-tangent line stabilizer of $PGU(3, q)$ is lifted completely. Also we will show that any automorphism of \mathcal{X}_n is obtained in this way, yielding that \mathcal{X}_n has precisely $(q+1)q(q^2 - 1)m = q(q^2 - 1)(q^n + 1)$ automorphisms. Moreover, we show that even though $g(\mathcal{X}_n) = g(\mathcal{C}_n)$, the curve \mathcal{X}_n is not isomorphic to \mathcal{C}_n and cannot be Galois covered by the Hermitian curve \mathcal{H}_{q^n} if $q > 2$. Finally, we show that several new genera for $\mathbb{F}_{q^{2n}}$ -maximal curves can be obtained by considering some of the subcovers of \mathcal{X}_n .

2 The curves \mathcal{X}_n

The starting point of our generalization of the GK curve is to consider a different model of \mathcal{C} . This model also occurs in [12]. Let $\rho \in \mathbb{F}_{q^2}$ with $\rho^q + \rho = 1$, and consider the \mathbb{F}_{q^2} -projectivity φ associated to the matrix A where

$$A := \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 - \rho & 0 & 0 & -\rho \end{pmatrix}.$$

In terms of the affine coordinates X, Y, Z this amounts to the algebraic transformation

$$\varphi(X) = \frac{X+1}{(1-\rho)X-\rho}, \quad \varphi(Y) = \frac{Y}{(1-\rho)X-\rho}, \quad \text{and} \quad \varphi(Z) = \frac{-Z}{(1-\rho)X-\rho}.$$

Also using the variables X, Y , and Z for $\mathcal{X} := \varphi(\mathcal{C})$, we obtain that \mathcal{X} is given by the affine equations

$$\mathcal{X} : \begin{cases} Z^{q^2-q+1} = Y \frac{X^{q^2} - X}{X^{q+1} - 1} \\ Y^{q+1} = X^{q+1} - 1 \end{cases}.$$

Inspired by this, we consider for each odd n with $n \geq 3$, the algebraic curve \mathcal{X}_n given by the affine equations

$$\mathcal{X}_n : \begin{cases} Z^m = Y \frac{X^{q^2} - X}{X^{q+1} - 1} \\ Y^{q+1} = X^{q+1} - 1 \end{cases}, \quad (1)$$

where $m := (q^n + 1)/(q + 1)$. In particular, as for the construction in [9], we note that $\mathcal{X} = \mathcal{X}_3$, which we have seen to be isomorphic to \mathcal{C}_3 . As we will see later, for $n \geq 5$ the curves \mathcal{X}_n are new and in particular not isomorphic to \mathcal{C}_n . We start our investigation of the curves \mathcal{X}_n by computing their genera.

Proposition 2.1. *Let q be a power of a prime p and let $n \geq 5$ odd. Then the genus of \mathcal{X}_n is given by*

$$g(\mathcal{X}_n) = g(\mathcal{C}_n) = \frac{(q-1)(q^{n+1} + q^n - q^2)}{2}.$$

Proof. Let $\mathbb{F}_{q^{2n}}(x, y)$ be the function field defined by $y^{q+1} = x^{q+1} - 1$ and $\mathcal{H}_q : Y^{q+1} - X^{q+1} + 1$ be the Hermitian curve over \mathbb{F}_{q^2} as before. Seen as a projective curve, \mathcal{H}_q is nonsingular having $q+1$ infinite points, namely $Q_\infty^i = (1 : \alpha_i : 0)$ where $\alpha_i^{q+1} = 1$ for $i = 1, \dots, q+1$. Let P_∞^i with $i = 1, \dots, q+1$ be the place of $\mathbb{F}_{q^{2n}}(x, y)$ corresponding to the point Q_∞^i . Further, for $a \in \mathbb{F}_{q^{2n}}$ such that $a^{q+1} \neq 1$, let $P_{x=a}^1, \dots, P_{x=a}^{q+1}$ and $P_{y=0}^1, \dots, P_{y=0}^{q+1}$ be the places lying over $x = a$ in $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(x)$ and over $y = 0$ in $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(y)$ respectively. Then we have the following identities of divisors in $\mathbb{F}_{q^{2n}}(x, y)$,

$$(x-a)_{\mathbb{F}_{q^{2n}}(x,y)} = \sum_{j=1}^{q+1} P_{x=a}^j - \sum_{i=1}^{q+1} P_\infty^i, \quad \text{and} \quad (y)_{\mathbb{F}_{q^{2n}}(x,y)} = \sum_{j=1}^{q+1} P_{y=0}^j - \sum_{i=1}^{q+1} P_\infty^i.$$

This implies that

$$\begin{aligned} \left(y \frac{x^{q^2} - x}{x^{q+1} - 1} \right)_{\mathbb{F}_{q^{2n}}(x,y)} &= \sum_{i=1}^{q+1} P_{y=0}^i - \sum_{j=1}^{q+1} P_\infty^j + \sum_{\substack{a \in \mathbb{F}_{q^2}, \\ a^{q+1} \neq 1}} \sum_{k=1}^{q+1} P_{x=a}^k - (q^2 - q - 1) \sum_{j=1}^{q+1} P_\infty^j \\ &= \sum_{i=1}^{q+1} P_{y=0}^i + \sum_{\substack{a \in \mathbb{F}_{q^2}, \\ a^{q+1} \neq 1}} \sum_{k=1}^{q+1} P_{x=a}^k - (q^2 - q) \sum_{j=1}^{q+1} P_\infty^j. \end{aligned}$$

Thus, the support of the divisor of $y(x^{q^2} - x)/(x^{q+1} - 1)$ consists of $q^3 + 1$ places of $\mathbb{F}_{q^{2n}}(x, y)$, corresponding precisely to the \mathbb{F}_{q^2} -rational points of \mathcal{H}_q . The divisor of $y(x^{q^2} - x)/(x^{q+1} - 1)$ also shows that this function is not a d -th power of another function in $\mathbb{F}_{q^{2n}}(x, y)$ for any $d > 1$. Hence $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(x, y)$ is a Kummer extension of degree m . The standard theory of Kummer extensions, see for example [20, Proposition 3.7.3], implies that the $q^3 + 1$ places occurring in the divisor of $y(x^{q^2} - x)/(x^{q+1} - 1)$ are precisely the ramified places of $\mathbb{F}_{q^{2n}}(x, y)$ in the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(x, y)$. Moreover all these places are totally ramified. Using the Riemann–Hurwitz formula and the fact that $g(\mathbb{F}_{q^{2n}}(x, y)) = q(q-1)/2$, yields

$$2g(\mathbb{F}_{q^{2n}}(x, y, z)) - 2 = m(q(q-1) - 2) + (m-1)(q^3 + 1).$$

Hence for $n \geq 3$ odd, we obtain

$$g(\mathcal{X}_n) = g(\mathbb{F}_{q^{2n}}(x, y, z)) = \frac{(q-1)(q^{n+1} + q^n - q^2)}{2} = g(\mathcal{C}_n).$$

□

The following corollary is a direct consequence of Proposition 2.1 and a result from [7].

Corollary 2.2. *Let $n \geq 3$ be an odd integer and suppose $q \geq 3$. Then the curve \mathcal{X}_n defined in Equation (1), is not a Galois subcover of the Hermitian curve \mathcal{H}_{q^n} .*

Proof. In [7] it was shown that for $q \geq 3$ and $n \geq 3$ odd, the curve \mathcal{C}_n is not a Galois subcover of the Hermitian curve \mathcal{H}_{q^n} . There, it was noted in a remark directly following [7, Proposition 5.1] that in fact for $q \geq 3$ a prime power and $n \geq 3$ an odd integer, *any* curve defined over $\mathbb{F}_{q^{2n}}$ of genus $g(\mathcal{C}_n) = (q-1)(q^{n+1} + q^n - q^2)/2$ is not a Galois subcover of the Hermitian curve \mathcal{H}_{q^n} . Hence the corollary follows from Proposition 2.1. □

Remark 2.3. *Proposition 2.1 and the similarity between the definitions of \mathcal{C}_n and \mathcal{X}_n may give rise to the suspicion that these curves are isomorphic over $\mathbb{F}_{q^{2n}}$. However, using the same projectivity φ as before, note that $\tilde{\mathcal{C}}_n = \varphi(\mathcal{C}_n)$ is given by the affine equations:*

$$\tilde{\mathcal{C}}_n : \begin{cases} Z^m = Y \frac{X^{q^2} - X}{X^{q+1} - 1} (X - 1)^{m - (q^2 - q + 1)} \\ Y^{q+1} = X^{q+1} - 1 \end{cases}.$$

This shows that $\mathcal{X}_3 \cong \mathcal{C}_3$, which we already knew, but no obvious isomorphism between \mathcal{X}_n and \mathcal{C}_n can be derived for $n \geq 5$. As mentioned already, we will show later that in fact the curves \mathcal{X}_n and \mathcal{C}_n are not isomorphic if $n \geq 5$.

To complete the picture as to whether or not \mathcal{X}_n is a Galois subcover of \mathcal{H}_{q^n} , we also settle the case $q = 2$.

Lemma 2.4. *Let $n \geq 3$ odd and $q = 2$. Then \mathcal{X}_n is a Galois subcover of the Hermitian curve \mathcal{H}_{2^n} .*

Proof. For $q = 2$, Equation (1) reads:

$$\mathcal{X}_n : \begin{cases} Z^m = Y \frac{X^4 + X}{X^3 + 1} = XY \\ Y^3 = X^3 + 1 \end{cases},$$

providing a plane model for \mathcal{X}_n given by $\mathcal{Y}_n : Z^{2^n+1} = X^3(X^3 + 1)$. We claim that more generally for a prime power r , a plane curve \mathcal{Y} given by an affine equation $\mathcal{Y} : Z^{r+1} = X^h(X^h + 1)$ where $h \mid (r+1)$, is a Galois subcover of $\mathcal{H}_r : U^{r+1} - V^{r+1} + 1 = 0$. To see this, consider the rational map $\psi : \mathcal{H}_r \rightarrow \mathcal{Y}$, with $\psi(U, V) = (X, Z) = (U^{\frac{r+1}{h}}, UV)$. Indeed, we note that

$$Z^{r+1} - X^h(X^h + 1) = (UV)^{r+1} - U^{2(r+1)} - U^{r+1} = U^{r+1}(V^{r+1} - U^{r+1} - 1) = 0.$$

This proves the claim. Since 3 divides $2^n + 1$ for odd n , the lemma follows from the claim we just proved by applying it to the case $q = 2^n$ and $h = 3$. □

This lemma immediately implies that \mathcal{X}_n is $\mathbb{F}_{2^{2n}}$ -maximal, since it is a subcover of an $\mathbb{F}_{2^{2n}}$ -maximal curve. Lemma 2.4 also reveals a first difference between the curves \mathcal{C}_n and \mathcal{X}_n . Indeed, for $q = 2$, \mathcal{C}_3 was shown to be a Galois subcover of \mathcal{H}_{q^3} in [10], but in [11] it is proved that, for $q = 2$ and $n \geq 5$, \mathcal{X}_n is not a Galois subcover of \mathcal{H}_{q^n} . Combining the above, we see that for $q = 2$, the curves \mathcal{C}_n and \mathcal{X}_n are isomorphic if and only if $n = 3$. We now prove that the same holds for $q \geq 3$. This result will follow as an immediate corollary of the following theorem.

Theorem 2.5. *Let q be a prime power and $n \geq 3$ odd. Then $\text{Aut}(\mathcal{X}_n)$ contains a subgroup G with $G \cong SL(2, q) \rtimes C_{q^n+1}$, where C_k denotes a cyclic group of order k . Moreover, denoting by $\text{Fix}(G)$, the fixed field of G in $\mathbb{F}_{q^{2n}}(x, y, z)$, we have $\text{Fix}(G) = \mathbb{F}_{q^{2n}}(z^{q^n+1})$. Further, there exists a subgroup S of G with $S \cong SL(2, q) \times C_m$ and $\text{Fix}(S) = \mathbb{F}_{q^{2n}}(z^m) = \mathbb{F}_{q^{2n}}(y(x^{q^2} - x)/(x^{q+1} - 1))$.*

Proof. The Hermitian curve \mathcal{H}_q defined by the affine equation $Y^{q+1} = X^{q+1} - 1$ has, as we have noted already, $q+1$ points at infinity. These points lie on a non-tangent line ℓ . From [19] the stabilizer M_ℓ of a non-tangent line ℓ is a maximal subgroup of $\text{Aut}(\mathcal{H}_q)$ of order $q(q-1)(q+1)^2$. Moreover, M_ℓ is isomorphic to $S_\ell \rtimes C_{q+1}$ where C_{q+1} is a cyclic group of order $q+1$, and S_ℓ is the commutator subgroup of M_ℓ , which in turn is isomorphic to $SL(2, q)$. An explicit description of M_ℓ and S_ℓ is given in [19] in matrix representation as follows:

$$M_\ell = \left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} : a, b, c, d \in \mathbb{F}_{q^2}, d^{q+1} - b^{q+1} = 1, a^{q+1} - c^{q+1} = 1, -a^q b + c^q d = 0 \right\},$$

$$S_\ell = \left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix} \in M_\ell : ad - bc = 1 \right\} \cong SL(2, q),$$

also see [5, Sect. 3] for more details.

We will identify matrices from M_ℓ with their associated projectivities and denote with $\alpha_{a,b,c,d}$ the projectivity associated to the matrix in M_ℓ with entries a, b, c, d . Then for any $\alpha_{a,b,c,d} \in M_\ell$, we have that $c^q d = a^q b$,

$$1 + b^{q+1} = d^{q+1} = \frac{a^{q(q+1)} b^{q+1}}{c^{q(q+1)}} = \frac{(1 + c^{q+1})^q b^{q+1}}{c^{q(q+1)}} = \left(\frac{b}{c^q} \right)^{q+1} + b^{q+1},$$

and

$$d^{q+1} - 1 = b^{q+1} = \frac{c^{q(q+1)} d^{q+1}}{a^{q(q+1)}} = \frac{(-1 + a^{q+1})^q d^{q+1}}{a^{q(q+1)}} = -\left(\frac{d}{a^q} \right)^{q+1} + d^{q+1}.$$

This means that for any $\alpha_{a,b,c,d} \in M_\ell$ there exists $\zeta \in \mathbb{F}_{q^2}$ such that $\zeta^{q+1} = 1$, $b = \zeta c^q$, and $d = \zeta a^q$. In particular, this implies that $b = c^q$ and $a = d^q$ for every $\alpha_{a,b,c,d} \in S_\ell$. Hence we have shown that

$$M_\ell = \left\{ \begin{pmatrix} a & \zeta c^q & 0 \\ c & \zeta a^q & 0 \\ 0 & 0 & 1 \end{pmatrix} : a, c \in \mathbb{F}_{q^2}, a^{q+1} - c^{q+1} = 1, \zeta^{q+1} = 1 \right\} \quad (2)$$

and

$$S_\ell = \left\{ \begin{pmatrix} a & c^q & 0 \\ c & a^q & 0 \\ 0 & 0 & 1 \end{pmatrix} : a, c \in \mathbb{F}_{q^2}, a^{q+1} - c^{q+1} = 1 \right\}. \quad (3)$$

As before, denote by $\mathbb{F}_{q^{2n}}(x, y)$ the Hermitian function field over $\mathbb{F}_{q^{2n}}$ where $y^{q+1} - x^{q+1} + 1 = 0$. We are going to analyze the induced action on $\mathbb{F}_{q^{2n}}(x, y)$ of $\alpha_{a,b,c,d} \in M_\ell$, where $b = \zeta c^q$ and $d = \zeta a^q$. First of all, note that a direct computation gives that for any $\alpha_{a,b,c,d} \in M_\ell$ we have

$$\alpha_{a,b,c,d}(y)^{q+1} - \alpha_{a,b,c,d}(x)^{q+1} + 1 = y^{q+1} - x^{q+1} + 1.$$

Hence $\alpha_{a,b,c,d}$ is an automorphism of the function field $\mathbb{F}_{q^{2n}}(x, y)$ (as well as of the curve \mathcal{H}_q). Now consider the function $u := y(x^{q^2} - x)/(x^{q+1} - 1) = (x^{q^2} - x)/y^q$ in $\mathbb{F}_{q^{2n}}(x, y)$. Then we have

$$\alpha_{a,b,c,d}(u) = (cx + dy) \left(\frac{ax^{q^2} + by^{q^2} - ax - by}{(cx + dy)^{q+1}} \right) = \left(\frac{ax^{q^2} + by^{q^2} - ax - by}{c^q x^q + d^q y^q} \right).$$

Observe that

$$\begin{aligned} (x^{q^2} - x)(c^q x^q + d^q y^q) &= c^q x^{q^2+q} + d^q x^{q^2} y^q - c^q x^{q+1} - d^q y^q x \\ &= c^q (y^{q+1} + 1)^q + d^q x^{q^2} y^q - c^q (y^{q+1} + 1) - d^q y^q x \\ &= c^q y^{q^2+q} + d^q x^{q^2} y^q - c^q y^{q+1} - d^q y^q x \\ &= y^q (c^q y^{q^2} + d^q x^{q^2} - c^q y - d^q x). \end{aligned}$$

Combining this with Equation (2), we see that

$$\frac{\alpha_{a,b,c,d}(u)}{u} = \frac{y^q (ax^{q^2} + by^{q^2} - ax - by)}{(x^{q^2} - x)(c^q x^q + d^q y^q)} = \frac{ax^{q^2} + by^{q^2} - ax - by}{c^q y^{q^2} + d^q x^{q^2} - c^q y - d^q x} = \zeta,$$

where in the last equality we used that $b = \zeta c^q$ and $a = a^{q^2} = d^q / \zeta^q = \zeta d^q$. In particular Equation (3) now implies that $\alpha_{a,b,c,d}(u) = u$ if and only if $\alpha_{a,b,c,d} \in S_\ell$. Hence $u \in \text{Fix}(S_\ell)$ and $u^{q+1} \in \text{Fix}(M_\ell)$. On the other hand from the proof of Lemma 2.1, we see that the pole divisor of u has degree $q^3 - q = |S_\ell|$. Hence $[\mathbb{F}_{q^{2n}}(x, y) : \mathbb{F}_{q^{2n}}(u)] = |S_\ell|$ and $[\mathbb{F}_{q^{2n}}(x, y) : \mathbb{F}_{q^{2n}}(u^{q+1})] = (q+1)|S_\ell| = |M_\ell|$. This implies that $\mathbb{F}_{q^{2n}}(u) = \text{Fix}(S_\ell)$ and $\mathbb{F}_{q^{2n}}(u^{q+1}) = \text{Fix}(M_\ell)$.

Now let $\alpha_{a,b,c,d} \in M_\ell$, where $b = \zeta c^q$ and $d = \zeta a^q$. Since in $\mathbb{F}_{q^{2n}}(x, y, z)$ we have that $z^m = u$ and $\alpha_{a,b,c,d}(u) = \zeta u$, for any $\alpha_{a,b,c,d} \in M_\ell$ and $\xi \in \mathbb{F}_{q^{2n}}$ such that $\xi^m = \zeta$, the transformation $\alpha_{a,b,c,d,\xi} : (x, y, z) \mapsto (ax + by, cy + dy, \xi z)$ is an automorphism of $\mathbb{F}_{q^{2n}}(x, y, z)$. Note that since $\zeta^{q+1} = 1$, we have $\xi^{q^{n+1}} = 1$, implying that indeed $\xi \in \mathbb{F}_{q^{2n}}$. Hence the groups of transformations

$$G := \{\alpha_{a,\zeta c^q,c,\zeta a^q,\xi} : \alpha_{a,\zeta c^q,c,\zeta a^q} \in M_\ell, \xi^m = \zeta\} \quad (4)$$

and

$$S := \{\alpha_{a,c^q,c,a^q,\xi} : \alpha_{a,c^q,c,a^q} \in S_\ell, \xi^m = 1\} \quad (5)$$

are automorphism groups of \mathcal{X}_n with $G \cong SL(2, q) \rtimes C_{q^n+1}$ and $S \cong S_\ell \times C_m \cong SL(2, q) \times C_m$. Further $\text{Fix}(G) = \text{Fix}(M_\ell) = \mathbb{F}_{q^{2n}}(u^{q+1}) = \mathbb{F}_{q^{2n}}(z^{q^{n+1}})$ and $\text{Fix}(S) = \text{Fix}(S_\ell) = \mathbb{F}_{q^{2n}}(u) = \mathbb{F}_{q^{2n}}(z^m)$, since $[\mathbb{F}_{q^{2n}}(x, y, z) : K(z^{q^{n+1}})] = |M_\ell|m = |G|$ and $[\mathbb{F}_{q^{2n}}(x, y, z) : K(z^m)] = |S_\ell|m = |S|$. \square

Corollary 2.6. *Let q be a prime power and $n \geq 3$ odd. Then \mathcal{X}_n is isomorphic to \mathcal{C}_n if and only if $n = 3$.*

Proof. We already know that \mathcal{C}_3 and \mathcal{X}_3 are isomorphic. Now assume that $n \geq 5$. From Theorem 2.5, we have that $q(q-1)(q+1)(q^n+1)$ divides $|\text{Aut}(\mathcal{X}_n)|$ while from [13, 14], we know that $|\text{Aut}(\mathcal{C}_n)| = q^3(q-1)(q^n+1) = q^3(q-1)(q^n+1)$. Since $q(q-1)(q+1)(q^n+1)$ does not divide $q^3(q-1)(q^n+1)$ we conclude that \mathcal{X}_n is not isomorphic to \mathcal{C}_n . \square

Remark 2.7. *The proof of Theorem 2.5 directly implies several facts on certain function field extensions and their corresponding Galois groups: the field extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(z^{q^{n+1}})$ is Galois with Galois group isomorphic to the group G given in Equation (4). Similarly, the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(z^m)$ is*

Galois with Galois group isomorphic to the group S given in Equation (5). In the next section, we will also use the following subgroup of S :

$$\tilde{S} := \{\alpha_{a,c^q,c,a^q,1} : \alpha_{a,c^q,c,a^q} \in S_\ell\}, \quad (6)$$

which is directly seen to be the Galois group of the Galois extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(z)$. Indeed any element from \tilde{S} fixes z , while \tilde{S} has cardinality $|SL(2, q)| = q^3 - q = [\mathbb{F}_{q^{2n}}(x, y, z) : \mathbb{F}_{q^{2n}}(z)]$, since it is isomorphic to the group S_ℓ from Equation (3), which in turn was isomorphic to $SL(2, q)$. Finally note that the Theorem 2.5 directly implies that group S_ℓ is the Galois group of the Galois extension $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(u)$, with $u = y(x^{q^2} - x)/(x^{q+1} - 1)$.

3 \mathcal{X}_n is $\mathbb{F}_{q^{2n}}$ -maximal for every $n \geq 5$ odd

In this section we prove that the algebraic curves \mathcal{X}_n are $\mathbb{F}_{q^{2n}}$ -maximal for any q and $n \geq 3$ odd. The proof proceeds in several steps, proving the maximality of certain key subfields of $\mathbb{F}_{q^{2n}}(x, y, z)$ first, before showing the maximality of $\mathbb{F}_{q^{2n}}(x, y, z)$ itself. An overview of the various function fields is given in Figure 1. Some of the stated extension degrees and equations may not be clear at this point, but will be explained later in this section.

Lemma 3.1. *Let $\mathbb{F}_{q^{2n}}(x, y)$ be as before defined by $y^{q+1} - x^{q+1} + 1 = 0$ and define $\rho := x + y$, $\delta := \rho^{q^2-1}$. Then $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(\rho)$ is an Artin-Schreier extension of degree q and $\mathbb{F}_{q^{2n}}(\rho)/\mathbb{F}_{q^{2n}}(\delta)$ is a Kummer extension of degree $q^2 - 1$.*

Proof. The statement that $\mathbb{F}_{q^{2n}}(\rho)/\mathbb{F}_{q^{2n}}(\delta)$ is a Kummer extension of degree $q^2 - 1$ is trivial and we therefore only prove the first statement. As in the previous section denote by P_∞^i , $i = 1, \dots, q+1$, the places of $\mathbb{F}_{q^{2n}}(x, y)$ corresponding to the “infinite” points $Q_\infty^i = (1 : \alpha_i : 0)$ on the algebraic curve $Y^{q+1} - X^{q+1} + 1 = 0$. We make the convention that $Q_\infty^1 = (1 : -1 : 0)$. Since Q_∞^1 is a point of the polar line of $(0 : 0 : 1)$ at \mathcal{H}_q , the Reciprocity Law of polarities yields that $(0 : 0 : 1)$ is a point of the polar line of Q_∞^1 which is the tangent line of \mathcal{H}_q at Q_∞^1 . Thus, the line $X + Y = 0$ intersects \mathcal{H}_q at Q_∞^1 with multiplicity $q + 1$. Hence

$$(\rho)_{\mathbb{F}_{q^{2n}}(x, y)} = (x + y)_{\mathbb{F}_{q^{2n}}(x, y)} = (q + 1)P_\infty^1 - \sum_{i=1}^{q+1} P_\infty^i = qP_\infty^1 - \sum_{i=2}^{q+1} P_\infty^i. \quad (7)$$

This shows that $[\mathbb{F}_{q^{2n}}(x, y) : \mathbb{F}_{q^{2n}}(\rho)] = q$. To find an algebraic relation between ρ and x , note that $\rho^{q+1} = x^{q+1} + y^{q+1} + x^q y + xy^q = 2x^{q+1} - 1 + x^q y + xy^q = x^q \rho + x \rho^q - 1$, and hence

$$\left(\frac{x}{\rho}\right)^q + \left(\frac{x}{\rho}\right) = \frac{\rho^{q+1} + 1}{\rho^{q+1}}. \quad (8)$$

This implies that the extension $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(\rho)$ is an Artin-Schreier extension. \square

Remark 3.2. *It is not hard to describe the Galois group of the extension $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(\rho)$ as a subgroup of the group M_ℓ from Equation (2). Indeed, from Equation (8) we see that an automorphism σ of $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(\rho)$ sends x/ρ to $x/\rho + \alpha$ with α satisfying $\alpha^q + \alpha = 0$. In terms of x and y , we obtain*

$$\sigma(x) = \rho \cdot \left(\frac{x}{\rho} + \alpha\right) = (\alpha + 1)x + \alpha y \quad \text{and} \quad \sigma(y) = \rho - \sigma(x) = -\alpha x + (1 - \alpha)y.$$

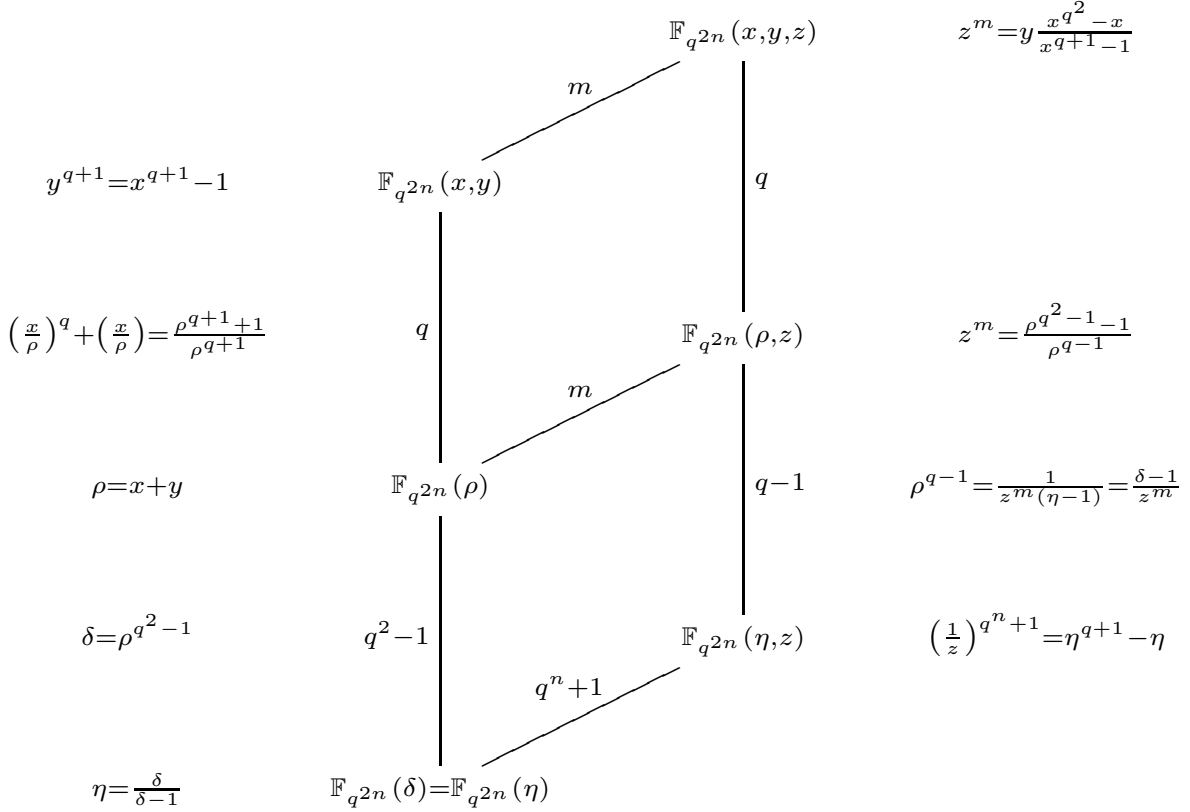


Figure 1: An overview of several subfields of $\mathbb{F}_{q^{2n}}(x, y, z)$.

Hence the group of such automorphisms σ can be identified with the Sylow p -subgroup of S_ℓ given by

$$S_{\ell, q} = \left\{ \begin{pmatrix} 1 + \alpha & \alpha & 0 \\ -\alpha & 1 - \alpha & 0 \\ 0 & 0 & 1 \end{pmatrix} : \alpha^q + \alpha = 0 \right\}.$$

We now turn our attention to the function field $\mathbb{F}_{q^{2n}}(\eta, z)$ from Figure 1, where $\eta := \delta/(\delta - 1)$. Note that $\delta = \eta/(\eta - 1)$, implying that $\mathbb{F}_{q^{2n}}(\eta) = \mathbb{F}_{q^{2n}}(\delta)$. First we determine the genus of $\mathbb{F}_{q^{2n}}(\eta, z)$.

Lemma 3.3. *Let $\delta := \rho^{q^2-1}$ and $\eta := \delta/(\delta - 1)$. Then the extension $\mathbb{F}_{q^{2n}}(\eta, z)/\mathbb{F}_{q^{2n}}(\eta)$ is a Kummer extension of degree $q^n + 1$. The function field $\mathbb{F}_{q^{2n}}(\eta, z)$ has genus $g(\mathbb{F}_{q^{2n}}(\eta, z)) = \frac{1}{2}(m - 1)(q + 1)$.*

Proof. We will start the proof by finding an algebraic relation between z and δ . First of all, note that since

$\rho = x + y$ and $y^{q+1} = x^{q+1} - 1$, we have that

$$\begin{aligned} y^{q+1}(\rho^{q^2} - \rho) &= y^{q+1}(x^{q^2} - x) + (x^{q+1} - 1)(y^{q^2} - y) \\ &= y^{q+1}(x^{q^2} - x) + (x^{q+1} - 1)y((y^{q+1})^{q-1} - 1) \\ &= y^{q+1}(x^{q^2} - x) + (x^{q+1} - 1)y((x^{q+1} - 1)^{q-1} - 1) \\ &= y^{q+1}(x^{q^2} - x) + y(x^{q^2+q} - x^{q+1}) = \rho^q y(x^{q^2} - x). \end{aligned}$$

Hence

$$z^m = \frac{y(x^{q^2} - x)}{x^{q+1} - 1} = \frac{x^{q^2} - x}{y^q} = \frac{\rho^{q^2} - \rho}{\rho^q} = \frac{\rho^{q^2-1} - 1}{\rho^{q-1}}. \quad (9)$$

Since $\delta = \rho^{q^2-1}$, taking the $q+1$ -th power on both sides of the above equation shows that

$$z^{q^n+1} = \frac{(\delta - 1)^{q+1}}{\delta}.$$

Hence in terms of $\eta = \delta/(\delta - 1)$, we obtain that

$$\left(\frac{1}{z}\right)^{q^n+1} = \frac{\delta}{(\delta - 1)^{q+1}} = \eta^{q+1} - \eta. \quad (10)$$

This shows that $\mathbb{F}_{q^{2n}}(\eta, z)/\mathbb{F}_{q^{2n}}(\eta)$ is a Kummer extension of degree $q^n + 1$. The genus now follows directly from the theory of Kummer extensions: the two zeroes of $\eta^{q+1} - \eta = \eta(\eta - 1)^q$ are totally ramified, while there are $q + 1$ places of $\mathbb{F}_{q^{2n}}(\eta, z)$ above the pole of $\eta^{q+1} - \eta$, each with ramification index m , since the pole order $q + 1$ divides the extension degree $q^n + 1$. Applying the Riemann-Hurwitz genus formula to the extension $\mathbb{F}_{q^{2n}}(\eta, z)/\mathbb{F}_{q^{2n}}(\eta)$ we obtain

$$2g(\mathbb{F}_{q^{2n}}(\eta, z)) - 2 = (q^n + 1)(-2) + 2q^n + (q + 1)(m - 1).$$

The desired result now follows directly. \square

We now prove maximality of the function field $\mathbb{F}_{q^{2n}}(\eta, z)$. The essential ingredient of the proof is to use a Galois-descent-type argument by interpreting $\mathbb{F}_{q^{2n}}$ as a 2-dimensional space over \mathbb{F}_{q^n} .

Proposition 3.4. *Let q be a prime power and $n \geq 3$ odd. The function field $\mathbb{F}_{q^{2n}}(\eta, z)$ where $z^{q^n+1} = \eta^{q+1} - \eta$, is $\mathbb{F}_{q^{2n}}$ -maximal.*

Proof. Using Lemma 3.3, the theorem is equivalent with the statement that the function field $\mathbb{F}_{q^{2n}}(\eta, z)$ has precisely

$$q^{2n} + 1 + (q + 1)(m - 1)q^n = q + 3 + (q^n + 1)(q^n - 2 + q^n - q)$$

many $\mathbb{F}_{q^{2n}}$ -rational places. Above the poles and zeroes of $\eta^{q+1} - \eta$ in $\mathbb{F}_{q^{2n}}(\eta)$ lie exactly $2 + q + 1$ $\mathbb{F}_{q^{2n}}$ -rational places of $\mathbb{F}_{q^{2n}}(\eta, z)$. Further, for any $\eta \in \mathbb{F}_{q^n} \setminus \{0, 1\}$, the equation $z^{q^n+1} = \eta^{q+1} - \eta$ has $q^n + 1$ distinct solutions in $\mathbb{F}_{q^{2n}}$, since then $\eta^{q+1} - \eta \in \mathbb{F}_{q^n} \setminus \{0\}$. This gives rise to precisely $q^n - 2$ places of $\mathbb{F}_{q^{2n}}(\eta)$ that split completely in the extension $\mathbb{F}_{q^{2n}}(\eta, z)/\mathbb{F}_{q^{2n}}(\eta)$. What remains to be shown is that there exist $q^n - q$ values of $\eta \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ such that the equation $z^{q^n+1} = \eta^{q+1} - \eta$ has $q^n + 1$ distinct solutions in $\mathbb{F}_{q^{2n}}$. Equivalently, we need to show that there are $q^n - q$ values of $\eta \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ such that $\eta^{q+1} - \eta \in \mathbb{F}_{q^n} \setminus \{0\}$.

Now fix $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and suppose that $\eta \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$. Since n is odd, any element $\eta \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$ can uniquely be written in the form $\eta = \eta_1 + \alpha\eta_2$, with $\eta_1, \eta_2 \in \mathbb{F}_{q^n}$ and $\eta_2 \neq 0$. Now note that

$$\begin{aligned} \eta^{q+1} - \eta &= (\eta_1 + \alpha\eta_2)^{q+1} - (\eta_1 + \alpha\eta_2) \\ &= \eta_1^{q+1} + \eta_1^q \alpha \eta_2 + \eta_1 \alpha^q \eta_2^q + \alpha^{q+1} \eta_2^{q+1} - \eta_1 - \alpha\eta_2 \\ &= \eta_1^{q+1} + \eta_1(\alpha^q + \alpha)\eta_2^q + \alpha^{q+1} \eta_2^{q+1} - \eta_1 + \alpha(\eta_1^q \eta_2 - \eta_1 \eta_2^q - \eta_2). \end{aligned}$$

This implies that $\eta^{q+1} - \eta \in \mathbb{F}_{q^n} \setminus \{0\}$ if and only if $\eta_1^q \eta_2 - \eta_1 \eta_2^q - \eta_2 = 0$. Since we require that $\eta_2 \neq 0$, we obtain that

$$\eta_1^q - \eta_1 \eta_2^{q-1} - 1 = 0 \quad \text{or equivalently} \quad \eta_2^{q-1} = \frac{(\eta_1 - 1)^q}{\eta_1}. \quad (11)$$

Now we compute the number of possibilities for (η_1, η_2) by considering above equation as a defining equation of a function field $\mathbb{F}_{q^n}(\eta_1, \eta_2)$. By Equation (11), the extension $\mathbb{F}_{q^n}(\eta_1, \eta_2)/\mathbb{F}_{q^n}(\eta_1)$ is a Kummer extension of degree $q-1$ in which the zeroes of η_1 and $\eta_1 - 1$ in $\mathbb{F}_{q^n}(\eta_1)$ are totally ramified with ramification index $q-1$, while the pole of η_1 in $\mathbb{F}_{q^n}(\eta_1)$ splits completely. This implies that the genus of $\mathbb{F}_{q^n}(\eta_1, \eta_2)$ is zero and hence that it has $q^n + 1$ many \mathbb{F}_{q^n} -rational places. Of these, exactly $q+1$ are either a pole of η_2 (equivalently a pole or zero of η_1) or a zero of $\eta_1 - 1$. This leaves $q^n - q$ many \mathbb{F}_{q^n} -rational places of $\mathbb{F}_{q^n}(\eta_1, \eta_2)$. Each of these places give rise to a distinct value of $\eta \in \mathbb{F}_{q^{2n}}$ satisfying that $\eta_2 \neq 0$, while $\eta^{q+1} - \eta \in \mathbb{F}_{q^n}^*$. This is what we needed to show. \square

Corollary 3.5. *For a given $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, a place P of $\mathbb{F}_{q^{2n}}(\delta)$ splits completely in the extension $\mathbb{F}_{q^{2n}}(\eta, z)/\mathbb{F}_{q^{2n}}(\eta)$ if and only the evaluation $\delta(P)$ of δ at P satisfies:*

1. $\delta(P) \in \mathbb{F}_{q^n} \setminus \{0, 1\}$, or
2. $\delta(P) = \frac{1 + \alpha t^q}{t^{q-1}(1 + \alpha t)}$, for $t \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$.

Proof. From the proof of Proposition 3.4 we see that a splitting place P comes about in two ways.

If $\eta(P)$ is in $\mathbb{F}_{q^n} \setminus \{0, 1\}$, then, since $\delta = \eta/(\eta - 1)$, we have $\delta(P) \in \mathbb{F}_{q^n} \setminus \{0, 1\}$.

If $\eta(P) = \eta_1 + \alpha\eta_2$ where $\eta_1, \eta_2 \in \mathbb{F}_{q^n}$, $\eta_2 \neq 0$ and $\eta_1^q - \eta_1 \eta_2^{q-1} - 1 = 0$, then we define $t := \frac{\eta_2}{\eta_1 - 1}$. Using Equation (11), we can express η_1 and η_2 in terms of t yielding that

$$\eta(P) = \eta_1 + \alpha\eta_2 = \frac{1}{1 - t^{q-1}} + \alpha \frac{t^q}{1 - t^{q-1}} = \frac{1 + \alpha t^q}{1 - t^{q-1}}.$$

Hence

$$\delta(P) = \frac{\eta(P)}{\eta(P) - 1} = \frac{1 + \alpha t^q}{1 - t^{q-1}} \cdot \frac{1 - t^{q-1}}{1 + \alpha t^q + t^{q-1} - 1} = \frac{1 + \alpha t^q}{t^{q-1}(1 + \alpha t)}.$$

Recall from the proof of Proposition 3.4 that the zero and pole of η_1 as well as the zero of $\eta_1 - 1$ should not be considered when studying completely splitting places. Since $\eta_1 = 1/(1 - t^{q-1})$, this means that $t \in \mathbb{F}_{q^n}$, but $t \notin \mathbb{F}_q$ just as claimed. \square

To prove the maximality of \mathcal{X}_n , or equivalently of $\mathbb{F}_{q^{2n}}(x, y, z)$, the strategy is now to study which of the places in Corollary 3.5 split completely in the extension $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(\delta)$ as well. Indeed, in light of Figure 1, such places will also split completely in the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(\delta)$, since it is the composite of $\mathbb{F}_{q^{2n}}(x, y)$ and $\mathbb{F}_{q^{2n}}(\delta, z)$. We will first consider the extension $\mathbb{F}_{q^{2n}}(\rho)/\mathbb{F}_{q^{2n}}(\delta)$.

The description of the splitting places in the previous corollary seems to depend on the choice of $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. However, note that the set of splitting places as a whole does not depend on α . The same is true for the set of splitting places in the next proposition.

Proposition 3.6. *For a given $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, let P be a place of $\mathbb{F}_{q^{2n}}(\delta)$ such that the evaluation $\delta(P)$ of δ at P satisfies:*

1. $\delta(P) \in (\mathbb{F}_{q^n})^{q-1} \setminus \{0, 1\}$, or
2. $\delta(P) = \frac{1 + \alpha t^q}{t^{q-1}(1 + \alpha t)}$, for $t \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$.

Then the place P splits completely in the function field extension $\mathbb{F}_{q^{2n}}(\rho)/\mathbb{F}_{q^{2n}}(\delta)$.

Proof. Since $\delta = \rho^{q^2-1}$, it is clear that the equation $\rho^{q^2-1} = \delta(P)$ has $q^2 - 1$ distinct solutions in $\mathbb{F}_{q^{2n}}$ if $\delta(P)$ is a $(q - 1)$ -th power in \mathbb{F}_{q^n} . Since $\delta(P) \notin \{0, 1\}$ by Corollary 3.5, the first part of the proposition follows.

Now suppose that $\delta(P) = \frac{1 + \alpha t^q}{t^{q-1}(1 + \alpha t)}$, for $t \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. To see that $\delta(P)$ is a $(q^2 - 1)$ -th power in \mathbb{F}_{q^n} , observe that since $t \in \mathbb{F}_{q^n}$, then t^{q-1} is a $(q^2 - 1)$ -th power in $\mathbb{F}_{q^{2n}}$. Hence, δ is a $(q^2 - 1)$ -th power in $\mathbb{F}_{q^{2n}}$ if and only if $(1 + \alpha t^q)/(1 + \alpha t)$ is. Since $t^{q^{2n+1}} = t^q$ and $\alpha^{q^2} = \alpha$ we have that

$$(1 + \alpha t^q) = (1 + \alpha t^{q^{2n-1}})^{q^2} = (1 + \alpha t^{q^{2n-1}})^{q^2-1} (1 + \alpha t^{q^{2n-1}}).$$

Similarly,

$$(1 + \alpha t^{q^{2n-1}}) = (1 + \alpha t^{q^{2n-3}})^{q^2} = (1 + \alpha t^{q^{2n-3}})^{q^2-1} (1 + \alpha t^{q^{2n-3}})$$

and proceeding iteratively, we obtain

$$(1 + \alpha t^{2n-(n-2)}) = (1 + \alpha t^{q^n})^{q^2} = (1 + \alpha t^{q^n})^{q^2-1} (1 + \alpha t^{q^n}) = (1 + \alpha t^{q^n})^{q^2-1} (1 + \alpha t).$$

This shows that

$$\delta = \frac{1}{t^{q-1}} \cdot \left(\prod_{\substack{1 \leq i \leq n \\ i \text{ odd}}} (1 + \alpha t^{q^{2n-i}}) \right)^{q^2-1} \cdot \frac{1 + \alpha t}{1 + \alpha t} = \frac{1}{t^{q-1}} \cdot \left(\prod_{\substack{1 \leq i \leq n \\ i \text{ odd}}} (1 + \alpha t^{q^{n-i}}) \right)^{q^2-1}, \quad (12)$$

which implies the desired. \square

Corollary 3.7. *The function field $\mathbb{F}_{q^{2n}}(\rho, z)$ given by the equation $z^m = \frac{\rho^{q^2-1}-1}{\rho^{q-1}}$ is an $\mathbb{F}_{q^{2n}}$ -maximal function field of genus $g(\mathbb{F}_{q^{2n}}(\rho, z)) = \frac{1}{2}(m-1)(q^2-1)$.*

Proof. The extension $\mathbb{F}_{q^{2n}}(\rho, z)/\mathbb{F}_{q^{2n}}(\rho)$ is a Kummer extension of degree m in which precisely $q^2 + 1$ places ramify, namely the q^2 zeroes of $\rho^{q^2} - \rho$ and the pole of ρ . Moreover, all these places are totally ramified and $\mathbb{F}_{q^{2n}}$ -rational. Hence by the Riemann–Hurwitz genus formula, we obtain the genus of $\mathbb{F}_{q^{2n}}(\rho, z)$ directly.

To prove the maximality, we need to show that apart from the q^2 zeroes of $\rho^{q^2} - \rho$ and the pole of ρ in $\mathbb{F}_{q^{2n}}(\rho, z)$, the function field $\mathbb{F}_{q^{2n}}(\rho, z)$ contains a further

$$q^{2n} + 1 + q^n(m-1)(q^2-1) - q^2 - 1 = m(q^2-1) \left(\frac{q^n - q}{q-1} + q^n - q \right)$$

$\mathbb{F}_{q^{2n}}$ -rational places. However, combining Corollary 3.5 and Proposition 3.6, we see that exactly $(q^n - q)/(q - 1) + q^n - q$ places of $\mathbb{F}_{q^{2n}}(\delta)$ split completely in the extension $\mathbb{F}_{q^{2n}}(\rho, z)/\mathbb{F}_{q^{2n}}(\delta)$, since $\mathbb{F}_{q^{2n}}(\rho, z)$ is the composite of $\mathbb{F}_{q^{2n}}(\rho)$ and $\mathbb{F}_{q^{2n}}(\eta, z)$; see Figure 1. \square

The following corollary is a direct consequence of the proofs of the previous results and among others describes the splitting places in the extension $\mathbb{F}_{q^{2n}}(\rho, z)/\mathbb{F}_{q^{2n}}(\rho)$. It will be useful to prove the maximality of $\mathbb{F}_{q^{2n}}(x, y, z)$.

Corollary 3.8. *Let $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be given. The $\mathbb{F}_{q^{2n}}$ -rational places of $\mathbb{F}_{q^{2n}}(\rho, z)$ lie above the following three types of places of $\mathbb{F}_{q^{2n}}(\rho)$:*

1. *The $q^2 + 1$ totally ramified places of $\mathbb{F}_{q^{2n}}(\rho)$ in $\mathbb{F}_{q^{2n}}(\rho, z)/\mathbb{F}_{q^{2n}}(\rho)$. More specifically, these are the q^2 places P in $\mathbb{F}_{q^{2n}}(\rho)$ such that $\rho^{q+1}(P) \in \mathbb{F}_q$ together with the pole of ρ in $\mathbb{F}_{q^{2n}}(\rho)$.*
2. *The $(q+1)(q^n - q)$ places P of $\mathbb{F}_{q^{2n}}(\rho)$ satisfying that $\rho^{q+1}(P) \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. These places split completely in $\mathbb{F}_{q^{2n}}(\rho, z)/\mathbb{F}_{q^{2n}}(\rho)$.*
3. *The $(q^2 - 1)(q^n - q)$ places P of $\mathbb{F}_{q^{2n}}(\rho)$ satisfying that*

$$\rho^{q+1}(P) = \frac{a}{t} \cdot \left(\prod_{j=0}^n (1 + \alpha^{q^{j+1}} t^{q^{n-j}}) \right),$$

for some $a \in \mathbb{F}_q \setminus \{0\}$ and $t \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. These places split completely in $\mathbb{F}_{q^{2n}}(\rho, z)/\mathbb{F}_{q^{2n}}(\rho)$.

Proof. Apart from item 3., this follows directly from Proposition 3.6 and Corollary 3.7, since $\delta = \rho^{q^2-1}$. To derive the expression in the third type of places, observe that Equation (12) implies that

$$\rho^{q+1}(P) = \frac{a}{t} \cdot \left(\prod_{\substack{1 \leq i \leq n \\ i \text{ odd}}} (1 + \alpha t^{q^{n-i}}) \right)^{q+1} = \frac{a}{t} \cdot \left(\prod_{j=0}^n (1 + \alpha^{q^{j+1}} t^{q^{n-j}}) \right),$$

with $a \in \mathbb{F}_q \setminus \{0\}$. In the second equality, we used that $\alpha \in \mathbb{F}_{q^2}$ and hence $\alpha^{q^2} = \alpha$ as well as that $t \in \mathbb{F}_{q^n}$. \square

Now we prove the main result of this section.

Theorem 3.9. *Let q be a prime power and $n \geq 3$ an odd integer. The curve \mathcal{X}_n with function field $\mathbb{F}_{q^{2n}}(x, y, z)$ defined by $y^{q+1} = x^{q+1} - 1$ and $z^m = y(x^{q^2} - x)/(x^{q+1} - 1)$, is an $\mathbb{F}_{q^{2n}}$ -maximal curve.*

Proof. By Proposition 2.1, the maximality of \mathcal{X}_n follows, if we can show that $\mathbb{F}_{q^{2n}}(x, y, z)$ has precisely the following number of $\mathbb{F}_{q^{2n}}$ -rational places:

$$q^{2n} + 1 + q^n(q-1)(q^{n+1} + q^n - q^2) = 1 + q^3 + 1 + mq \left((q+1)(q^n - q) + (q^2 - 1)(q^n - q) \right). \quad (13)$$

It is easy to see that the $q^2 + 1$ places of type 1. from Corollary 3.8 gives rise to exactly $q^3 + 1$ $\mathbb{F}_{q^{2n}}$ -rational places of $\mathbb{F}_{q^{2n}}(x, y)$ (indeed, these places correspond exactly to the $q^3 + 1$ \mathbb{F}_{q^2} -rational points of the Hermitian curve \mathcal{H}_q). All these $q^3 + 1$ places are totally ramified in the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(x, y)$. Hence maximality of $\mathbb{F}_{q^{2n}}(x, y, z)$ follows if we can show that the remaining $(q+1)(q^n - q) + (q^2 - 1)(q^n - q)$ places of $\mathbb{F}_{q^{2n}}(\rho)$ from Corollary 3.8, split completely in the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(\rho)$; also see Figure 1.

Recall Equation (8) describing the extension $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(\rho)$ explicitly as an Artin-Schreier extension:

$$\left(\frac{x}{\rho} \right)^q + \left(\frac{x}{\rho} \right) = \frac{\rho^{q+1} + 1}{\rho^{q+1}};$$

also see Figure 1. If P is one of the $(q+1)(q^n - q)$ places of $\mathbb{F}_{q^{2n}}(\rho)$ satisfying that $\rho^{q+1}(P) \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$, then $(\rho^{q+1}(P) + 1)/\rho^{q+1}(P) \in \mathbb{F}_{q^n}$. By Equation (8), we see that P splits completely in the extension $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(\rho)$. Since by Corollary 3.8, the place P also splits completely in $\mathbb{F}_{q^{2n}}(\rho, z)/\mathbb{F}_{q^{2n}}(\rho)$, we conclude that P also splits completely in $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(\rho)$, since $\mathbb{F}_{q^{2n}}(x, y, z)$ is the compositum of $\mathbb{F}_{q^{2n}}(\rho, z)$ and $\mathbb{F}_{q^{2n}}(x, y)$.

Now suppose that P is one of the $(q^2 - 1)(q^n - q)$ places of $\mathbb{F}_{q^{2n}}(\rho)$ satisfying that

$$\rho^{q+1}(P) = \frac{a}{t} \cdot \left(\prod_{j=0}^n (1 + \alpha^{q^{j+1}} t^{q^{n-j}}) \right),$$

for some $a \in \mathbb{F}_q \setminus \{0\}$ and $t \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. The theorem is proved, if we can show the claim that these places all split completely in the extension $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(\rho)$. Since

$$T^{q^{2n}} - T = \sum_{\ell=0}^{2n-1} (-1)^\ell (T^q + T)^{q^\ell},$$

the equation $T^q + T = \frac{\rho^{q+1}(P)+1}{\rho^{q+1}(P)}$ has q solutions in $\mathbb{F}_{q^{2n}}$ if and only if

$$\sum_{\ell=0}^{2n-1} (-1)^\ell \left(\frac{\rho^{q+1}(P)+1}{\rho^{q+1}(P)} \right)^{q^\ell} = 0,$$

or equivalently, if and only if

$$\sum_{\ell=0}^{2n-1} (-1)^\ell \left(\frac{1}{\rho^{q+1}(P)} \right)^{q^\ell} = 0. \quad (14)$$

Let $A := \prod_{j=0}^{n-1} (1 + \alpha^{q^j} t^{q^{n-j}})$, so that $\rho^{q+1}(P) = \frac{a}{t} \cdot A^{q^n} \cdot (1 + \alpha t)$ and hence $\frac{1}{\rho^{q+1}(P)} = b \cdot \frac{A \cdot t}{1 + \alpha t}$ for some $b \in \mathbb{F}_q \setminus \{0\}$. Here we used that $A^{q^{n+1}} = \prod_{j=0}^{2n-1} (1 + \alpha^{q^j} t^{2n-j}) \in \mathbb{F}_q \setminus \{0\}$, since

$$\left(A^{q^{n+1}} \right)^q = \prod_{j=0}^{2n-1} (1 + \alpha^{q^{j-1}} t^{2n-j+1}) = A^{q^n+1}.$$

Since $b \in \mathbb{F}_q \setminus \{0\}$, Equation (14) can then be rewritten as

$$\sum_{\ell=0}^{2n-1} (-1)^\ell \left(\frac{t \cdot A}{1 + \alpha t} \right)^{q^\ell} = 0. \quad (15)$$

Observe that

$$A = t^{1+q+\dots+q^{n-1}} \cdot (t^{-1} + \alpha) \cdot (t^{-q^{n-1}} + \alpha^q) \cdot \dots \cdot (t^{-q} + \alpha),$$

where $t^{1+q+\dots+q^{n-1}} \in \mathbb{F}_q \setminus \{0\}$, since $t \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. Writing $1 + \alpha t = (\alpha + t^{-1})t$ and denoting $s := t^{-1}$, we see that Equation (15) is equivalent to

$$\sum_{\ell=0}^{2n-1} (-1)^\ell \left(\prod_{j=0}^{n-2} (s^{q^{j+1}} + \alpha^{q^j}) \right)^{q^\ell} = 0. \quad (16)$$

Since the choice of α is arbitrary as long as the condition $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is satisfied, we may replace α with α^q , and correspondingly replace Equation (16) by the equivalent equation

$$\sum_{\ell=0}^{2n-1} (-1)^\ell \left(\prod_{j=0}^{n-2} (s^{q^j} + \alpha^{q^j}) \right)^{q^\ell} = \sum_{\ell=0}^{2n-1} (-1)^\ell (s + \alpha)^{q^\ell \cdot \frac{q^{n-1}-1}{q-1}} = 0. \quad (17)$$

for $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and all $s \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. In other words, the theorem will follow if we can show that the polynomial

$$P(T) := \sum_{\ell=0}^{2n-1} (-1)^\ell T^{q^\ell \cdot \frac{q^{n-1}-1}{q-1}}$$

vanishes for all values of the form $T = s + \alpha$, where $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $s \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. Observe that for any such value of $T = s + \alpha$, we have $T^{q^{2n}} - T = 0$ and $T^{q^n} - T - c = 0$, where $c := \alpha^q - \alpha \in \mathbb{F}_{q^2}$ satisfies $c^q + c = 0$. Therefore, we may simplify the condition $P(T) = 0$ by replacing $P(T)$ with any polynomial that is equivalent to it modulo the polynomials $T^{q^{2n}} - T$ and $T^{q^n} - T - c$. Concretely, we will use this to replace $P(T)$ by a polynomial of lower degree. First of all, for $\ell \geq n+1$ we have

$$q^\ell \frac{q^{n-1}-1}{q-1} = q^\ell \frac{q^{2n-\ell}-1}{q-1} + q^{2n} \frac{q^{\ell-n-1}-1}{q-1}.$$

Hence working modulo $T^{q^{2n}} - T$ the condition $P(T) = 0$ can be simplified to

$$\bar{P}(T) = \sum_{\ell=0}^n (-1)^\ell T^{q^\ell \frac{q^{n-1}-1}{q-1}} + \sum_{\ell=n+1}^{2n-1} (-1)^\ell T^{q^\ell \frac{q^{2n-\ell}-1}{q-1} + \frac{q^{\ell-n-1}-1}{q-1}} = 0.$$

Similarly working modulo $T^{q^n} - T - c$ and using that $(-1)^n = -1$, the condition $\bar{P}(T) = 0$ can be simplified to

$$\begin{aligned} 0 &= T^{\frac{q^{n-1}-1}{q-1}} + \sum_{\ell=1}^n (-1)^\ell T^{\frac{q^n-q^\ell}{q-1}} (T+c)^{\frac{q^{\ell-1}-1}{q-1}} + \sum_{\ell=n+1}^{2n-1} (-1)^\ell T^{\frac{q^{\ell-n-1}-1}{q-1}} (T+c)^{\frac{q^n-q^{\ell-n}}{q-1}} \\ &= \sum_{\ell=1}^n (-1)^\ell T^{\frac{q^n-q^\ell}{q-1}} (T+c)^{\frac{q^{\ell-1}-1}{q-1}} - \sum_{\ell=1}^n (-1)^\ell (T+c)^{\frac{q^n-q^\ell}{q-1}} T^{\frac{q^{\ell-1}-1}{q-1}}. \end{aligned} \quad (18)$$

Now let us write

$$P_1(T) = \sum_{\ell=1}^n (-1)^\ell T^{\frac{q^n-q^\ell}{q-1}} (T+c)^{\frac{q^{\ell-1}-1}{q-1}} \text{ and } P_2(T) = \sum_{\ell=1}^n (-1)^\ell (T+c)^{\frac{q^n-q^\ell}{q-1}} T^{\frac{q^{\ell-1}-1}{q-1}},$$

then what we need to show is that $P_1(T) = P_2(T)$ for any $T = s + \alpha$, where $\alpha^q - \alpha = c$ and $s \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. What we in fact will show is the stronger statement that $P_1(T) = P_2(T)$ as polynomials in T for any $c \in \mathbb{F}_{q^2}$ such that $c^q + c = 0$. The original claim about the splitting of places in the extension $\mathbb{F}_{q^{2n}}(x, y)/\mathbb{F}_{q^{2n}}(\rho)$ (and hence the theorem) will then follow as well.

At this point note that

$$\begin{aligned} (T+c)^{\frac{q^{\ell-1}-1}{q-1}} &= (T+c)^{1+q+\dots+q^{\ell-2}} = \prod_{j \in \{0, \dots, \ell-2\}} (T^{q^j} + c^{q^j}) \\ &= \sum_{I \subset \{0, \dots, \ell-2\}} \left(\prod_{j \in I} T^{q^j} \right) \left(\prod_{k \in \{0, \dots, \ell-2\} \setminus I} c^{q^k} \right), \end{aligned}$$

where the summation is over all subsets I of $\{0, \dots, \ell-2\}$. Hence

$$P_1(T) = \sum_{\ell=1}^n (-1)^\ell \sum_{I \subset \{0, \dots, \ell-2\}} T^{q^{n-1} + \dots + q^\ell} \left(\prod_{j \in I} T^{q^j} \right) \left(\prod_{k \in \{0, \dots, \ell-2\} \setminus I} c^{q^k} \right).$$

Similarly,

$$P_2(T) = \sum_{\ell'=1}^n (-1)^{\ell'} \sum_{J \subset \{\ell', \dots, n\}} \left(\prod_{j \in J} T^{q^j} \right) \left(\prod_{k \in \{\ell', \dots, n\} \setminus J} c^{q^k} \right) T^{q^{\ell'-2} + \dots + 1}.$$

Given ℓ and $I \subset \{0, \dots, \ell-2\}$, define $\ell' \geq 1$ to be the unique maximal integer such that $\{0, \dots, \ell'-2\} \subset I$. The case $\ell' = 1$ corresponds to the case that $0 \notin I$. Then $\ell' \leq \ell$, the case $\ell' = \ell$ corresponding to the case that $I = \{0, \dots, \ell-2\}$. Now, still for a given ℓ and $I \subset \{0, \dots, \ell-2\}$, define $J = \{\ell, \dots, n-1\} \cup (I \setminus \{0, \dots, \ell'-2\})$. Note that $J \subset \{\ell', \dots, n\}$, since by definition of ℓ' , the integer $\ell' - 1$ is not in I . Then we have

$$\begin{aligned} &(-1)^\ell T^{q^{n-1} + \dots + q^\ell} \left(\prod_{j \in I} T^{q^j} \right) \left(\prod_{k \in \{0, \dots, \ell-2\} \setminus I} c^{q^k} \right) = \\ &(-1)^\ell \frac{c^{q^{\ell'-1}}}{c^{q^{\ell-1}}} \left(\prod_{j \in J} T^{q^j} \right) \left(\prod_{k \in \{\ell', \dots, n\} \setminus J} c^{q^k} \right) T^{q^{\ell'-2} + \dots + 1} = \\ &(-1)^{\ell'} \left(\prod_{j \in J} T^{q^j} \right) \left(\prod_{k \in \{\ell', \dots, n\} \setminus J} c^{q^k} \right) T^{q^{\ell'-2} + \dots + 1}, \end{aligned}$$

where in the last equality we used that $c^{q^{\ell'-1}} = (-1)^{\ell-\ell'} c^{q^{\ell-1}}$, since $c^q = -c$. Summing this equality over $1 \leq \ell \leq n$ and all subsets $I \subset \{0, \dots, \ell-1\}$, we obtain that $P_1(T) = P_2(T)$ as claimed. \square

4 Determination of the full automorphism group of \mathcal{X}_n , $n \geq 5$

We will now determine the complete automorphism group of \mathcal{X}_n for $n \geq 5$. We already observed in Theorem 2.5 that $\text{Aut}(\mathcal{X}_n)$ contains a subgroup G , given in Equation (4), isomorphic to $SL(2, q) \rtimes C_{q^n+1}$. The group G is obtained lifting in m ways the maximal subgroup $M_\ell \cong SL(2, q) \rtimes C_{q+1}$ of $\text{Aut}(\mathcal{H}_q) \cong PGU(3, q)$ fixing the non-tangent line $\ell : X + Y = 0$. The aim of this section is to prove that for $n \geq 5$, G is the full

automorphism group of \mathcal{X}_n , implying also that M_ℓ is the largest subgroup $Aut(\mathcal{H}_q)$ that can be lifted to $Aut(\mathcal{X}_n)$, i.e., that $PGU(3, q)$ can be lifted if and only if $n = 3$. The following lemma describes the strategy that will be used to show that G is the full automorphism group of \mathcal{X}_n . The affine equations in (1) give rise to an affine part of the curve \mathcal{X}_n . Considering its projective closure, $q+1$ points of \mathcal{X}_n at infinity appear. The places of $\mathbb{F}_{q^{2n}}(x, y, z)$ corresponding to these will be denoted by $R_\infty^1, \dots, R_\infty^{q+1}$ and will be called the infinite places of $\mathbb{F}_{q^{2n}}(x, y, z)$. Moreover, we denote their restrictions to $\mathbb{F}_{q^{2n}}(x, y)$ by $P_\infty^1, \dots, P_\infty^{q+1}$, consistent with the previous notation. Finally recall that we assumed that place P_∞^1 is centered around the point $(1 : -1 : 0)$, implying that R_∞^1 is centered around the infinite point $(1 : -1 : 0 : 0)$ of \mathcal{X}_n .

Lemma 4.1. *Let $C_m = Gal(\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(x, y))$. If $Aut(\mathcal{X}_n)$ acts on the set $\Omega = \{R_\infty^1, \dots, R_\infty^{q+1}\}$ of the $q+1$ infinite places of $\mathbb{F}_{q^{2n}}(x, y, z)$, then $Aut(\mathcal{X}_n) = G$.*

Proof. From the proof of Lemma 2.1, the place P_∞^i is totally ramified in the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(x, y)$. Moreover, by definition, the place R_∞^i lies above it. Hence C_m fixes each of the places $R_\infty^1, \dots, R_\infty^{q+1}$. Let

$$T := \{\alpha \in Aut(\mathcal{X}_n) : \alpha(P) = P, \text{ for every } P \in \Omega\}.$$

Clearly, C_m is a subgroup of T .

We claim that T is a normal subgroup of $Aut(\mathcal{X}_n)$. Indeed, let $\alpha \in T$, $\beta \in Aut(\mathcal{X}_n)$ and $R_\infty^i \in \Omega$. Since $Aut(\mathcal{X}_n)$ acts on Ω , we have $\beta(R_\infty^i) = R_\infty^j$ for some $j = 1, \dots, q+1$. Thus, $\beta^{-1}\alpha\beta(R_\infty^i) = \beta^{-1}\alpha(R_\infty^j) = \beta^{-1}(R_\infty^j) = R_\infty^i$. Hence $\beta^{-1}\alpha\beta$ fixes Ω pointwise for every $\alpha \in T$ and $\beta \in Aut(\mathcal{X}_n)$. This proves the claim.

We now claim that the characteristic p does not divide $|T|$. If it did, then T would contain an element of order p , which by definition would fix the $q+1$ places in Ω . On the other hand, Theorem 3.9 implies that \mathcal{X}_n has zero p -rank. Then [16, Lemma 11.129] implies that any automorphism of order p cannot have more than one fixed place. This proves the second claim.

Thus, T is a normal subgroup of $Aut(\mathcal{X}_n)$ of order coprime with p , whose elements fix more than one place. This implies that T is cyclic using [16, Theorem 11.49]. Let $\beta \in Aut(\mathcal{X}_n)$ be chosen arbitrary and consider the conjugate $\beta^{-1}C_m\beta = C_m^\beta$. Then C_m^β is a cyclic subgroup of T of order m . Since T is cyclic and C_m is contained in T , we have that $C_m^\beta = C_m$. This shows that $C_m^\beta = C_m$ for every $\beta \in Aut(\mathcal{X}_n)$ and hence that $Aut(\mathcal{X}_n) = N_{Aut(\mathcal{X}_n)}(C_m)$.

Consider the quotient group $\tilde{G} = Aut(\mathcal{X}_n)/C_m$. Then \tilde{G} is a subgroup of $Aut(\mathcal{H}_q) \cong PGU(3, q)$ acting on the $q+1$ infinite places $P_\infty^1, \dots, P_\infty^{q+1}$ of $\mathbb{F}_{q^{2n}}(x, y)$ with $R_\infty^i|P_\infty^i$ for every $i = 1, \dots, q+1$. This implies that \tilde{G} is contained in the stabilizer M_ℓ of the non-tangent line ℓ and hence $|\tilde{G}|$ divides $q(q-1)(q+1)^2$, see [16, Theorem A.10]. Note that $G/C_m \leq \tilde{G}$ and hence $|\tilde{G}| \geq |G|/m = q(q-1)(q+1)^2$. Hence $|\tilde{G}| = q(q-1)(q+1)^2$ and $\tilde{G} = G/C_m$. Moreover, it shows that $|Aut(\mathcal{X}_n)| = |\tilde{G}| \cdot |C_m| = |G|$ and hence that $Aut(\mathcal{X}_n) = G$. \square

The aim of the rest of this section is to prove that $Aut(\mathcal{X}_n)$ acts on the set $\Omega = \{R_\infty^1, \dots, R_\infty^{q+1}\}$, since then the previous lemma implies that $Aut(\mathcal{X}_n) = G$. We will consider Weierstrass semigroups $H(R)$ of various $\mathbb{F}_{q^{2n}}$ -rational places R of $\mathbb{F}_{q^{2n}}(x, y, z)$ in order to achieve this. Since G contains a group acting transitively on Ω , it is sufficient to show that $H(R_\infty^1) \neq H(R)$ for every $i = 1, \dots, q+1$ and $R \in \mathcal{X}_n(\mathbb{F}_{q^{2n}}) \setminus \Omega$, where, as before, R_∞^1 denotes the place centered at the infinite point $(1 : -1 : 0 : 0)$. We will use also the notation $G(R)$ for the set of gaps of a place R , i.e., $G(R) := \mathbb{N} \setminus H(R)$.

Lemma 4.2. *Let $P \in \mathcal{X}_n(\mathbb{F}_{q^{2n}}) \setminus \Omega$. Then $mq^2 + mq + q^2 - q \in G(P)$ while $mq^2 + mq + q^2 - q \in H(P_\infty^i)$ for every $i = 1, \dots, q+1$. In particular $H(P) \neq H(P_\infty^i)$ for every $i = 1, \dots, q+1$ and $Aut(\mathcal{X}_n)$ acts on Ω .*

Proof. To prove that $mq^2 + mq + q^2 - q \in H(R_\infty^i)$ for every $i = 1, \dots, q+1$, it is sufficient to show that $mq, mq + q^2 - q \in H(R_\infty^1)$. Let P_∞^1 denote the restriction of R_∞^1 to $\mathbb{F}_{q^{2n}}(x, y)$. Equation (7) implies that

$$(\rho)_{\mathbb{F}_{q^{2n}}(x, y, z)} = qmR_\infty^1 - m \sum_{i=2}^{q+1} R_\infty^i,$$

so that $1/\rho$ has a pole of order mq at R_∞^1 and no poles elsewhere. Hence $mq \in H(R_\infty^1)$. Moreover,

$$(z)_{\mathbb{F}_{q^{2n}}(x, y, z)}^{(\infty)} = (q^2 - q) \sum_{i=1}^{q+1} R_\infty^i,$$

where $(z)_{\mathbb{F}_{q^{2n}}(x, y, z)}^{(\infty)}$ denotes the pole divisor of z . Hence,

$$\left(\frac{z}{\rho}\right)_{\mathbb{F}_{q^{2n}}(x, y, z)}^{(\infty)} = (qm + q^2 - q)R_\infty^1.$$

Here we used that $m - q^2 + q > 0$ as $n \geq 3$. Hence $mq + q^2 - q \in H(R_\infty^1)$.

We now prove that $mq^2 + mq + q^2 - q \in G(R)$ for every $R \in \mathcal{X}_n(\mathbb{F}_{q^{2n}}) \setminus \Omega$. To do that it is sufficient to show that there exists a regular (sometimes also called holomorphic) differential ω such that $v_R(\omega) = mq^2 + mq + q^2 - q - 1$, see [21, Corollary 14.2.5]. In the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(z)$ the unique ramified place is the pole of z above which lie the places in Ω . Moreover the group G contains a subgroup of order $q+1$ acting sharply transitively on Ω , while fixing z and dz , so $\text{supp}(dz) = \Omega$. Since $\deg(dz) = 2g(\mathcal{X}_n) - 2$ and $|\Omega| = q+1$, we get that

$$(dz)_{\mathbb{F}_{q^{2n}}(x, y, z)} = \frac{2g(\mathcal{X}_n) - 2}{q+1}(R_\infty^1 + \dots + R_\infty^{q+1}) = (q^{n+1} - q^n - q^2 + 2q - 2)(R_\infty^1 + \dots + R_\infty^{q+1}).$$

Hence the differential $f dz$ is regular if and only if $f \in L((q^{n+1} - q^n - q^2 + 2q - 2)(R_\infty^1 + \dots + R_\infty^{q+1}))$. In order to prove that $mq^2 + mq + q^2 - q \in G(R)$ it is therefore sufficient to construct a function $f \in L((q^{n+1} - q^n - q^2 + 2q - 2)(R_\infty^1 + \dots + R_\infty^{q+1}))$ such that $v_R(f) = mq^2 + mq + q^2 - q - 1$.

From Theorem 3.9 \mathcal{X}_n is $\mathbb{F}_{q^{2n}}$ -maximal and hence from the Fundamental Equation [16, Theorem 9.79], there exists a function t_R such that $(t_R)_{\mathbb{F}_{q^{2n}}(x, y, z)} = (q^n + 1)(R - R_\infty^1)$. In particular,

$$(t_R \cdot \rho)_{\mathbb{F}_{q^{2n}}(x, y, z)} = (q^n + 1)(R - R_\infty^1) + qmR_\infty^1 - m \sum_{i=2}^{q+1} R_\infty^i = (q^n + 1)R - m \sum_{i=1}^{q+1} R_\infty^i.$$

Moreover, since $R \in \mathcal{X}_n(\mathbb{F}_{q^{2n}}) \setminus \Omega$, R is centered at a certain affine point, say (a, b, c) with $a, b, c \in \mathbb{F}_{q^{2n}}$. Observe that $(z - c) \geq -(q^2 - q)(R_\infty^1 + \dots + R_\infty^{q+1})$ and since in the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(z)$ only the pole of z is ramified, we have $v_R(z - c) = 1$. Let $f = (t_R \cdot \rho)^q (z - c)^{q^2 - q - 1}$, then

$$(f)_{\mathbb{F}_{q^{2n}}(x, y, z)} \geq -(mq + (q^2 - q)(q^2 - q - 1))(R_\infty^1 + \dots + R_\infty^{q+1}).$$

Observing that $mq + (q^2 - q)(q^2 - q - 1) < q^{n+1} - q^n - q^2 + 2q - 2$, since $n \geq 5$, we get that $f \in L((q^{n+1} - q^n - q^2 + 2q - 2)(R_\infty^1 + \dots + R_\infty^{q+1}))$ and hence that $f dz$ is a regular differential. Moreover,

$$v_R(f dz) = v_R(f d(z - c)) = q(q^n + 1) + q^2 - q - 1 = (q^2 + q)m + q^2 - q - 1.$$

Considering the differential $w = f dz$ we obtain that $mq^2 + mq + q^2 - q \in G(R)$. \square

Combining the previous results the full automorphism group of \mathcal{X}_n has now been determined.

Theorem 4.3. *Let q be a prime power and $n \geq 5$ odd. The full automorphism group of \mathcal{X}_n is $\text{Aut}(\mathcal{X}_n) = G \cong SL(2, q) \rtimes C_{q^n+1}$. Moreover, $\text{Aut}(\mathcal{X}_n)$ has a non-tame short orbit Ω consisting of the $q+1$ infinite places of $\mathbb{F}_{q^{2n}}(x, y, z)$.*

Remark 4.4. *$\text{Aut}(\mathcal{X}_n)$ is asymptotically large, meaning that for every $q \geq 43$ and $n \geq 5$, the Classical Hurwitz upper bound $84(g(\mathcal{X}_n) - 1)$ does not hold.*

Remark 4.5. *We have seen that $\mathcal{C}_3 \cong \mathcal{X}_3$ and that for any q and any odd $n \geq 5$, the curves \mathcal{C}_n and \mathcal{X}_n have the same genus. One could suspect that if $n \geq 5$, the curves \mathcal{C}_n and \mathcal{X}_n , though not isomorphic, are twists of each other, i.e., are isomorphic over $\overline{\mathbb{F}}_q$. If this would be the case, their automorphism groups over $\overline{\mathbb{F}}_q$ would be identical. However, it was shown in [15, Thm. 3.10] that if \mathcal{K} is a maximal curve over \mathbb{F}_{q^2} of genus at least 2, then any automorphism of $\overline{\mathcal{K}}$, the curve obtained from \mathcal{K} by extending the field of definition to $\overline{\mathbb{F}}_q$, is already defined over \mathbb{F}_{q^2} . Since over $\mathbb{F}_{q^{2n}}$ and $n \geq 5$, the curves \mathcal{X}_n and \mathcal{C}_n have distinct automorphism groups, this result implies that they cannot be twists of each other.*

Though the previous results show that the curves \mathcal{X}_n for $n \geq 5$ exhibit different and new properties than previously known maximal curves, they do not provide examples of maximal curves with a previously unknown genus. In other words, these curves themselves do not add new values to the genus spectrum of maximal curves. Nevertheless, it is possible to provide new genera for maximal curves considering subfields of $\mathbb{F}_{q^{2n}}(x, y, z)$. As an example, in the following remark we consider some specific subfields of $\mathbb{F}_{q^{2n}}(x, y, z)$ with $n \geq 5$ which in some cases will produce (up to our knowledge) previously unknown values to this genus spectrum.

Remark 4.6. *Let q be a prime power and $n \geq 5$ odd. Let k_1 and k_2 be divisors of $q+1$ and $m = (q^n+1)/(q+1)$ respectively. The curve \mathcal{Y}_{k_1, k_2} with function field $\mathbb{F}_{q^{2n}}(w, s)$ defined by*

$$w^{\frac{q^n+1}{k_2}} = s^{\frac{q+1}{k_1}} \cdot \frac{(s^{\frac{q^2-1}{k_1}} - 1)^{q+1}}{(s^{\frac{q+1}{k_1}} - 1)^q}, \quad (19)$$

is $\mathbb{F}_{q^{2n}}$ -maximal of genus

$$g(\mathcal{Y}_{k_1, k_2}) = 1 + \frac{1}{2} \left[-\delta_1 - \frac{q+1}{k_1} + \frac{(q^2-1)(q^n+1)}{k_1 k_2} - \frac{q^2-1}{k_1} \delta_2 + \frac{q+1}{k_1} \delta_2 - \delta_3 \right], \quad (20)$$

where $k = (q^n+1)/k_2$, $\delta_1 = \gcd(k, \frac{q+1}{k_1})$, $\delta_2 = \gcd(k, q+1)$ and $\delta_3 = \gcd(k, \frac{q^2-1}{k_1})$. Moreover, \mathcal{Y}_{k_1, k_2} is a Galois subcover of \mathcal{X}_n of degree $k_1 \cdot k_2$.

Proof. Let H be the subgroup of the automorphism group of $\mathbb{F}_{q^{2n}}(x, y, z)$ generated by γ_{k_1} and γ_{k_2} , where

$$\gamma_{k_1} : (x, y, z) \mapsto (\lambda x, \lambda^{-1} y, z), \quad \gamma_{k_2} : (x, y, z) \mapsto (x, y, \xi z),$$

and $\lambda, \xi \in \mathbb{F}_{q^{2n}}$ with $\text{ord}(\lambda) = k_1$ and $\text{ord}(\xi) = k_2$. Then H is abelian of order $k_1 \cdot k_2$. More precisely, $H = C_{k_1} \times C_{k_2}$, where $C_{k_1} = \langle \gamma_{k_1} \rangle$ and $C_{k_2} = \langle \gamma_{k_2} \rangle$. Let $s = x^{k_1}$ and $w = z^{k_2}$. Then w and s are fixed by \mathcal{G} and

$$w^{\frac{q^n+1}{k_2}} = z^{q^n+1} = \frac{(x^{q^2} - x)^{q+1}}{(x^{q+1} - 1)^q} = s^{\frac{q+1}{k_1}} \cdot \frac{(s^{\frac{q^2-1}{k_1}} - 1)^{q+1}}{(s^{\frac{q+1}{k_1}} - 1)^q}.$$

This proves that $\mathbb{F}_{q^{2n}}(s, w) \subseteq \text{Fix}(H)$ and $w^{\frac{q^n+1}{k_2}} = s^{\frac{q+1}{k_1}} \cdot (s^{\frac{q^2-1}{k_1}} - 1)^{q+1} / (s^{\frac{q+1}{k_1}} - 1)^q$.

To show that the curve defined by Equation (19) is irreducible and to compute the genus of $\mathbb{F}_{q^{2n}}(s, w)$ we note that

$$\left(s^{\frac{q+1}{k_1}} \cdot \frac{(s^{\frac{q^2-1}{k_1}} - 1)^{q+1}}{(s^{\frac{q+1}{k_1}} - 1)^q} \right)_{\mathbb{F}_{q^{2n}}(s)} = \frac{(q+1)}{k_1} P_{s=0} + \sum_{\alpha \mid \frac{q+1}{k_1}=1} P_{s=\alpha} + (q+1) \cdot \sum_{\substack{\beta \mid \frac{q^2-1}{k_1}=1, \\ \beta \mid \frac{q+1}{k_1} \neq 1}} P_{s=\beta} - \frac{q(q^2-1)}{k_1} P_{s=\infty},$$

and hence $\mathbb{F}_{q^{2n}}(s, w)/\mathbb{F}_{q^{2n}}(s)$ is a Kummer extension of degree $k = (q^n + 1)/k_2$. From [20, Corollary 3.7.4],

$$\begin{aligned} g(\mathbb{F}_{q^{2n}}(s, w)) &= 1 - k + \frac{1}{2} \left[k - \delta_1 + \frac{q+1}{k_1}(k-1) + \left(\frac{q^2-1}{k_1} - \frac{q+1}{k_1} \right) (k - \delta_2) + k - \delta_3 \right] \\ &= 1 + \frac{1}{2} \left[-\delta_1 - \frac{q+1}{k_1} + \frac{(q^2-1)(q^n+1)}{k_1 k_2} - \frac{q^2-1}{k_1} \delta_2 + \frac{q+1}{k_1} \delta_2 - \delta_3 \right], \end{aligned}$$

where $\delta_1 = \gcd(k, \frac{q+1}{k_1})$, $\delta_2 = \gcd(k, q+1)$ and $\delta_3 = \gcd(k, \frac{(q^2-1)}{k_1})$.

In order to prove that $\mathbb{F}_{q^{2n}}(s, w) = \text{Fix}(H)$ consider the extension $\mathbb{F}_{q^{2n}}(x, y, z)/\mathbb{F}_{q^{2n}}(z^{q^n+1})$. Recall that from Theorem 2.5, $[\mathbb{F}_{q^{2n}}(x, y, z) : \mathbb{F}_{q^{2n}}(z^{q^n+1})] = |G| = (q^n + 1)q(q^2 - 1)$. Hence,

$$\begin{aligned} (q^n + 1)q(q^2 - 1) &= \\ [\mathbb{F}_{q^{2n}}(x, y, z) : \mathbb{F}_{q^{2n}}(s, w)] \cdot [\mathbb{F}_{q^{2n}}(s, w) : \mathbb{F}_{q^{2n}}(s, w^{\frac{q^n+1}{k_2}})] \cdot [\mathbb{F}_{q^{2n}}(s, w^{\frac{q^n+1}{k_2}}) : \mathbb{F}_{q^{2n}}(w^{\frac{q^n+1}{k_2}})] &= \\ [\mathbb{F}_{q^{2n}}(x, y, z) : \mathbb{F}_{q^{2n}}(s, w)] \cdot \frac{q^n+1}{k_2} \cdot \frac{q(q^2-1)}{k_1}, \end{aligned}$$

where the equality $[\mathbb{F}_{q^{2n}}(s, w^{\frac{q^n+1}{k_2}}) : \mathbb{F}_{q^{2n}}(w^{\frac{q^n+1}{k_2}})] = \frac{q(q^2-1)}{k_1}$ follows from Equation (19) observing that the degree in s equals $\frac{q+1}{k_1} + \frac{(q+1)(q^2-1)}{k_1} - \frac{q(q+1)}{k_1} = \frac{q(q^2-1)}{k_1}$. Thus, $[\mathbb{F}_{q^{2n}}(x, y, z) : \mathbb{F}_{q^{2n}}(s, w)] = k_1 \cdot k_2 = |H|$ and $\mathbb{F}_{q^{2n}}(s, w) = \text{Fix}(H)$. \square

Remark 4.6 provides new equations of $\mathbb{F}_{q^{2n}}$ -maximal curves for every q and $n \geq 5$ odd. Examples for small values of q and n are listed below. We have indicated a genus with boldface if it gives a new addition to the genus spectrum of $\mathbb{F}_{q^{2n}}$ -maximal curves. To check whether or not a genus gave a new addition, we compared our results with the genera of maximal function fields given in [1, 3, 4, 6, 8, 13, 18, 19].

- $q = 4$ and $n = 5$: $\{32, 156, \mathbf{302}, 1506, \mathbf{1532}\}$,
- $q = 4$ and $n = 7$: $\{\mathbf{212}, \mathbf{842}, 1056, 4206, \mathbf{24572}\}$,
- $q = 5$ and $n = 5$: $\{\mathbf{6242}, \mathbf{12484}, 18724\}$,
- $q = 7$ and $n = 5$: $\{\mathbf{243}, \mathbf{485}, 969, \mathbf{1941}, \mathbf{4563}, \mathbf{9125}, 18249, 36501, \mathbf{50403}, \mathbf{100805}, 201609\}$.

Acknowledgments

The second author would like to thank the Italian Ministry MIUR, Strutture Geometriche, Combinatoria e loro Applicazioni, Prin 2012 prot. 2012XZE22K and GNSAGA of the Italian INDAM.

References

- [1] M. Abdón, L. Quoos, *On the genera of subfields of the Hermitian function field*, Finite Fields Appl., **10**, 271-284, (2004).
- [2] M. Abdón, J. Bezerra and L. Quoos, *Further examples of maximal curves* J. Pure Appl. Algebra **213**, no. 6, 1192-1196, (2009).
- [3] N. Anbar, A. Bassa and P. Beelen, *A complete characterization of Galois subfields of the generalized Giulietti-Korchmáros function field*, Finite Fields Appl. **48**, 318-330, (2017).
- [4] A. Bassa, L. Ma, C. Xing and S.L. Yeo, *Towards a characterization of subfields of the Deligne-Lusztig function fields*, J. Combin. Theory Ser. A **120**, no. 7, 1351-1371, (2013).
- [5] A. Cossidente, G. Korchmáros and F. Torres, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra **28**, no. 10, 4707-4728, (2000).
- [6] Y. Danışman, M. Özdemir, *On the genus spectrum of maximal curves over finite fields*, J. Discr. Math. Sc. and Crypt. **18**, no.5, 513-529, (2015).
- [7] I. Duursma, K.H. Mak, *On maximal curves which are not Galois subcovers of the Hermitian curve* Bull. Braz. Math. Soc. **43**, no. 3, 453-465, (2012).
- [8] S. Fanali, M. Giulietti, *Quotient curves of the GK curve*, Adv. Geom. **12** no.2, 239-268, (2012).
- [9] A. Garcia, C. Güneri and H. Stichtenoth, *A generalization of the Giulietti-Korchmáros maximal curve*, Advances in Geometry **10**, no. 3, 427-434, (2010).
- [10] M. Giulietti, G. Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343**, 229-245, (2009).
- [11] M. Giulietti, M. Montanucci and G. Zini, *On maximal curves that are not quotients of the Hermitian curve*, Finite Fields Appl. **41**, 72-88, (2016).
- [12] M. Giulietti, L. Quoos and G. Zini, *Maximal curves from subcovers of the GK-curve*, J. Pure Appl. Algebra, **220**, no. 10, 3372-3383, (2016).
- [13] C. Güneri, M. Özdemir and H. Stichtenoth, *The automorphism group of the generalized Giulietti-Korchmáros function field*, Adv. Geom., **13**, 369-380, (2013).
- [14] R. Guralnick, B. Malmskog and R. Pries, *The automorphism group of a family of maximal curves*, J. Algebra, **361**, 92-106, (2012).
- [15] B. Gunby, A. Smith and A. Yuan, *Irreducible canonical representations in positive characteristic*, Res. Number Theory **1**, Art. 3, (2015).

- [16] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics*, Princeton, (2008).
- [17] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris **305**(Série I), 729-732, (1987).
- [18] L. Ma, C. Xing, *On subfields of the Hermitian function fields involving the involution automorphism*, preprint, arXiv:1707.07314.
- [19] M. Montanucci, G. Zini, *On the spectrum of genera of quotients of the Hermitian curve*, Comm. Algebra, DOI 10.1080/00927872.2018.1455100, (2018).
- [20] H. Stichtenoth, *Algebraic function fields and codes*, Springer, (2009).
- [21] G. D. Villa Salvador, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, (2006).

Peter Beelen
 Technical University of Denmark,
 Department of Applied Mathematics and Computer Science,
 Matematiktorvet 303B,
 2800 Kgs. Lyngby,
 Denmark,
 pabe@dtu.dk

Maria Montanucci
 Università degli Studi della Basilicata,
 Dipartimento di Matematica, Informatica ed Economia,
 Campus di Macchia Romana,
 Viale dell' Ateneo Lucano 10,
 85100 Potenza,
 Italy,
 maria.montanucci@unibas.it